2nd Nationwide Health Information Network Forum:
Health Information Network Security and Services
October 16-17, 2006
JW Marriott Pennsylvania Avenue

Forum Goals:

- Advance discussions and develop clarity on architecture approaches to ensure security and protect confidentiality
- Discuss the technical possibilities as well as the practical and policy implications of alternative architectural strategies in specific areas of health information networking.
- Share information on desired architectural characteristics and discuss possible paths to achieve them.
- Inform next steps in the advancement of the overall NHIN initiative, the work of the National Committee on Vital and Health Statistics on NHIN functional requirements, and considerations for necessary standards and eventual network certification.

Monday, October 16, 2006

8:00am – 9:00 am	Registration
9:00 am – 10:30am	Opening Plenary
10:30am – 10:45am	Break
10:45am – 12:00pm	Plenary Updates from Related Groups Report update from NCVHS Ad hoc NHIN WG
12:00pm – 1:15pm	Lunch
1:15pm – 2:30pm	Concurrent Sessions 1.1 Identifying the Services that could be provided by a Health Information Network Service Provider 1.2 Advancing NHIN Standards Needs through Use Case Elements
2:30pm – 2:45pm	Break
2:45pm – 4:00pm	Concurrent Panel Discussions 2.1 Approaches to Provider Authentication

There are different models for how health information network service providers may deal with authenticating care providers. In some models they authenticate organizations and not individuals. In some models, both individuals and organizations can be authenticated to take advantage of network services. In either model, managing who can access specific data in a particular care setting can be complicated by cross privileges referrals and access to provider identity information. This session will discuss the differing attributes of these different models and the various needs for sharing provider identity information.

2.2 Confidentiality and Secondary Use of Data

.

Uses of EHR data for population health management must respect the protection of patient confidentiality. At the same time the data needs of secondary uses span a spectrum from completely HIPAA de-identified data to state mandated reporting of patients with dangerous communicable diseases.

This session will discuss architectural strategies for enabling secondary uses of data including include anonymization, re-linkable anonymization, de-identification and selective data perturbation.

4:00pm - 5:15pm Concurrent Panel Discussions

3.1 Patient-driven access control

Many consumers want to decide who can access their health data and when they can do so. While policies for supporting both consumer data management and clinician needs to know are an active discussion area, architectures for patient management of data access need to be considered. In a networked health care environment, opportunities for patient management of access may exist in many places. These points of management may include where providers access PHR data, where there are look-ups and exchange of EHR data between organizations, and through patient driven access controls that may be asserted for use inside of care organizations. This session will discuss alternative architectural approaches for supporting consumer driven access controls and the type of

information that needs to be exchanged to make role based access controls operative at different points in a networked health system. Discussion will include practical aspects of existing role based access control.

3.2 Documenting Clinical Context

Health information networking will make information from PHR's and external organization's EHR's available to support patient care. The ability to identify the data context of clinical decisions can be important in understanding clinical history and supporting the rationale for previous clinical decisions. There are several architectural variations which could potentially support appropriate data persistence and/or recording of context. Approaches include transient display of external clinical data on a query by query basis, documented records of retrieved data, and data populating a "local" EHR. Different approaches may have implications for describing what was known and when. This session will focus on different approaches to dealing with retrieved data, how the approaches can provide varying levels of capability and what implications they may have for subsequent data retrievals as well.

5:30pm Adjourn

Tuesday, October 17, 2006

8:30am – 9:45am Concurrent Panel Discussions

4.1 Matching Patient Data

The need to correctly match patients with their data and data with their patients is a critical part of health information networking, but there are a number of factors that complicate approaches in this area. Protecting patient confidentiality, the quality and availability of patient indices, the different ways that newly generated data refer to patients, the complexities of data matching algorithms and variations in implementations in different systems are all complicating factors in meeting broader health networking needs. This session will focus on approaches for matching patient data without using a unique patient identifier, approaches to minimizing false positive and false negative patient data retrievals, issues of matching patient

data that is being delivered to a particular provider, and approaches to expressing the confidence level of matches and methods for refining possible matches. Practical experience with data matching with different levels of data reliability will also be discussed.

4.2 Accurate Attribution of Data

The value of clinical data is directly related to a level of assurance that the data are valid, reliably attributable and intact. Several methods for assuring data reliability are available including digital signatures and other mechanisms. Different approaches have different requirements and costs. Some approaches are document based and some work for non-document based data. There also may be different implications for a centralized vs. a distributed authentication environment. In this session, different approaches to supporting data reliability will be discussed as well as the practical aspects of implementation.

9:45am – 10:00am Break

10:00am – 11:15am Concurrent Panel Discussions

5.1 Auditing Data Access

Even when there is broad availability of role based access controls, networked health information exchange will bring substantial needs for auditing access to patient data. There are needs to record incoming access to EHR and PHR data, outgoing requests for data in a distributed authentication environment, and inter-organizational exchanges in the context of ongoing data connections and use. This session will discuss approaches to auditing in a complex networked care environment. Discussion will include what data needs to be exchanged and how it may need to flow to address these needs and others.

5.2 Information Distribution Approaches

While there has been a substantial focus on health information network functionality that can support data retrievals, there are also needs for source-initiated data distribution. “Pushed” data may be used to support, for

example, referrals, result reports, data updates and disease reporting. Two approaches for "pushing" data include "store and forward" data routing and "publish subscribe" methodologies. In this session, the different attributes and needs of these approaches will be discussed along with the needs that each has for provider identification, data addressing and authentication.

11:15am – 11:30pm Break

11:30pm – 12:30pm Closing Plenary and Public Comment